

# Summary of Delsarte's “Nombre de Solutions des Équations Polynomiales sur un Corps Fini”

Wim van Dam\*

February 1, 2008

## Abstract

An English summary is given of Jean Delsarte's article “Nombre de solutions des équations polynomiales sur un corps fini.”

## Introduction

These notes grew out of my desire to check the details of the article:

- Jean Delsarte, “Nombre de solutions des équations polynomiales sur un corps fini”, *Séminaire Bourbaki*, Exposé 39:1–9, March 1951

Because I was only interested in the main result, I did not translate the Sections 2 and 4. The same notation and equation numbering is maintained and the original page numbering is included in the right margin of the text. Some typos are corrected and I added some potentially helpful comments in italic. An alternative proof of the result of Delsarte was published in [2]. This paper cites both Delsarte and the 1949 article [1] by Elza Furtado Gomida as sources for the original result. I make this translation public to increase the accessibility of Delsarte's article. The current translation is by no means authoritative and does not contain any new results. Comments are welcome.

## References

- [1] Elza Furtado Gomida, “On the theorem of Artin-Weil”, *Boletim da Sociedade de Matemática de São Paulo*, Volume 4, pp. 1–18 (1949,1951)
- [2] Neal Koblitz, “The number of points on certain families of hypersurfaces over finite fields”, *Compositio Mathematica*, Volume 48, No. 1, pp. 3–23 (1983)

---

\*Massachusetts Institute of Technology, Center for Theoretical Physics, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, USA. email: vandam@mit.edu. This work is supported in part by funds provided by the U.S. Department of Energy and cooperative research agreement DF-FC02-94ER40818 and by a CMI postdoctoral fellowship.

# Number of Solutions of Polynomial Equations over Finite Fields

by Jean Delsarte

## 1 Gauss Sums of Finite Fields

Let  $K$  be a finite field  $\mathbb{F}_q$  and  $K^\times$  the multiplicative group  $\mathbb{F}_q^\times$ . Also, let  $\chi$  be a multiplicative character and  $\psi$  a non-trivial additive character. The Gauss sum over  $K$  is defined by

$$g(\chi) := \sum_{x \in K} \chi(x) \psi(x)$$

where the  $x$  could also run over  $K^\times$  as  $\chi(0) = 0$ . By changing  $x$  into  $tx$  with  $t \in K^\times$  we get

$$g(\chi) = \chi(t) \sum_{x \in K} \chi(x) \psi(tx),$$

which shows how to convert to different additive characters  $\psi$  by multiplying the Gauss sum by a known factor  $\chi(t)$ .

A classic result concerns the absolute value of the Gauss sum; we have

$$\begin{aligned} g(\chi) \bar{g}(\chi) &= \sum_{x \in K^\times} \sum_{y \in K^\times} \chi(xy^{-1}) \psi(x - y) \\ &= \sum_{x \in K^\times} \chi(x) \sum_{y \in K^\times} \psi((x - 1)y), \end{aligned}$$

where the summation over  $y \in K^\times$  is  $q - 1$  if  $x = 1$ , and  $-1$  otherwise. Thus

$$|g(\chi)| = \sqrt{q}.$$

## 2 Finite Extensions of Finite Fields: the Hasse-Davenport Theorem [...]

page 2

## 3 Some Enumerative Formulae

page 3

Let  $E_s$  be the  $s$ -dimensional  $K$  vector space  $K^s$ , view  $E_s$  as a ring with pointwise addition and multiplication. Consider the variety defined by the equation

$$\mathcal{F} := \sum_{i=1}^r a_i x_1^{m_{1i}} \cdots x_s^{m_{si}} = 0$$

with  $a_i \in K^0$  for  $i = 1, \dots, r$ . The size  $q$  of  $K$  is big, such that  $q - 1$  does not divide any of the  $m_{ij}$ . Let  $\psi$  be an additive character over  $K$ ; we want to calculate the summation  $S := \sum_x \psi(\mathcal{F}(x))$ , where the  $x = (x_1, \dots, x_s) \in E_s$ . We start by calculating the sum  $\bar{S}$  where we only sum over those  $x$  with  $x_j \in K^0$  (that is:  $x \in E_s^0$ ). Let

$$y_i = x_1^{m_{1i}} \dots x_s^{m_{si}}, \quad (1)$$

for  $i = 1, \dots, r$ , where  $x = (x_1, \dots, x_s)$  is an invertible element of the ring  $E_s = K \times \dots \times K$  ("Véronèse variety"). Equation 1 defines a group homomorphism from  $E_s^0$  to  $E_r^0$  (of the direct products of the multiplicative groups  $K^0$ ). Let  $d$  be the size of the kernel of this homomorphism and let  $G$  be its image; then we have

$$\bar{S} = \sum_{x \in E_s^0} \psi(\mathcal{F}(x)) = d \sum_{y \in G} \psi(ay) \quad (2)$$

with  $a = (a_1, \dots, a_r) \in E_r^0$  (the coefficients of  $\mathcal{F}$ ). The product  $ay$  is expressed in the ring  $E_r$  and the additive character  $\psi$  is extended to this ring (according to  $\psi(ay) := \psi(a_1 y_1 + \dots + a_r y_r) = \psi(a_1 y_1) \dots \psi(a_r y_r)$ ).

Let  $\chi$  be a multiplicative character of the group  $E_r^0$ ; we have for  $y = (y_1, \dots, y_r)$  in  $E_r^0$

$$\chi(y) = \chi_1(y_1) \dots \chi_r(y_r)$$

where  $(\chi_1, \dots, \chi_r)$  is a system of  $r$  multiplicative characters of  $K$ . Let us introduce the group  $\tilde{G}$  (orthogonal to  $G$ ), which is the ensemble of characters on  $E_r^0$  with  $\chi(y) = 1$  for every  $y \in G$ . Such a character is constant on the cosets of  $G$  in  $E_r^0$ . (The group  $\tilde{G}$  is the group of multiplicative characters on  $E_r^0/G$ ; hence its size is  $d(q-1)^{r-s}$ .) Now consider the sum

$$T = \sum_{\chi \in \tilde{G}} \sum_{y \in E_r^0} \chi(y) \psi(ay). \quad (3)$$

For fixed  $y$ , the sum  $\sum_{\chi}$  is zero when  $y$  is outside  $G$ , for  $y$  in  $G$  the sum is  $|\tilde{G}| = d(q-1)^{r-s}$ . Therefore

$$T = d(q-1)^{r-s} \sum_{y \in G} \psi(ay),$$

hence

$$T = (q-1)^{r-s} \bar{S},$$

and finally

$$\bar{S} = (q-1)^{s-r} \sum_{y \in \tilde{G}} \sum_{y \in E_r^0} \chi(y) \psi(ay). \quad (4)$$

Consider again the Gauss sums, which we have defined for  $K$  with an additive character  $\psi$ . For a multiplicative character  $\chi = (\chi_1, \dots, \chi_r)$  over  $E_r^0$ , define

$$\mathcal{G}(\chi) = g(\chi_1) \cdots g(\chi_r).$$

Because  $\psi(ay) = \psi(a_1 y_1) \cdots \psi(a_r y_r)$  we find (*because of the earlier derived equality*  $\sum_{y_j} \chi_j(y_j) \psi(a_j y_j) = \bar{\chi}_j(a_j) g(\chi_j)$ )

$$\sum_{y \in E_r^0} \chi(y) \psi(ay) = \bar{\chi}(a) \mathcal{G}(\chi) \quad (5)$$

and hence

$$\bar{S} = (q-1)^{s-r} \sum_{\chi \in \bar{G}} \bar{\chi}(a) \mathcal{G}(\chi). \quad (6)$$

**An application of the result.** Let us try to calculate the number of solutions of  $\mathcal{F} = 0$  in  $E_s^0$ , which gets denoted by  $\bar{N}$ . Let

$$\bar{S}(\psi) := \sum_{x \in E_s^0} \psi(\mathcal{F}(x))$$

Now calculate the sum of values  $\bar{S}(\psi)$  where  $\psi$  ranges over all non-trivial additive characters over  $K$ :

page 5

$$\sum_{\psi} \bar{S}(\psi) = \sum_{\psi} \sum_{x \in E_s^0} \psi(\mathcal{F}(x)).$$

For fixed  $x$ , the sum over the characters  $\psi$  will be  $-1$  if  $\mathcal{F}(x)$  is not 0, and  $q-1$  if  $\mathcal{F}(x) = 0$ , hence

$$\begin{aligned} \sum_{\psi} \bar{S}(\psi) &= (q-1)\bar{N} - ((q-1)^s - \bar{N}) \\ &= q\bar{N} - (q-1)^s \end{aligned}$$

because the number values  $x \in E_s^0$  for which  $\mathcal{F}(x) \neq 0$  is  $(q-1)^s - \bar{N}$ . Now fix a nontrivial character  $\psi_0$ . For every other nontrivial character  $\psi$  we have a  $u \in K^0$  such that  $\psi(x) = \psi_0(ux)$  for all  $x \in K$  (thus establishing a bijection between the set of nontrivial characters and  $K^0$ ). Moreover we have

$$g(\chi_1) = \sum_{x_1 \in K^0} \chi_1(x_1) \psi(x_1) = \sum_{x_1 \in K^0} \chi_1(x_1) \psi_0(ux_1),$$

or

$$g(\chi_1) = \bar{\chi}_1(u) g_0(\chi_1)$$

where  $g_0$  is the Gauss sum where we used the additive character  $\psi_0$ . Similarly, one finds

$$\mathcal{G}(\chi) = \lambda(u) \mathcal{G}_0(\chi),$$

for the Gauss sums over  $E_r$ . (Here  $\lambda$  is the multiplicative character over  $K^0$  defined by the product  $\lambda = \chi_1 \cdots \chi_r$ .) Finally, one gets

$$\bar{S}(\psi) = (q-1)^{s-r} \sum_{\chi \in \tilde{G}} \lambda(u) \bar{\chi}(a) \mathcal{G}_0(\chi).$$

If we want to sum this expression over all nontrivial  $\psi$ , it is sufficient to sum over all  $u \in K^0$ . If  $\chi$  is a multiplicative character over  $E_r^0$ , then for the character  $\lambda$  over  $K^0$ , we have that  $\sum_{u \in K^0} \lambda(u)$  is 0 if  $\lambda$  is nontrivial, and the sum is  $q-1$  if  $\lambda$  is trivial. We thus have

$$\sum_{\psi} \bar{S}(\psi) = (q-1)^{s-r+1} \sum_{\chi \in \tilde{G}^*} \chi(a) \mathcal{G}_0(\chi) \quad (7)$$

where  $\tilde{G}^*$  is the subgroup of  $\tilde{G}$  under the restriction that the product  $\chi_1 \cdots \chi_r$  is the trivial multiplicative character of  $K^0$ . “Without pain” we thus get the final result

$$\bar{N} = \frac{1}{q} \left[ (q-1)^s + (q-1)^{s-r+1} \sum_{\chi \in \tilde{G}^*} \bar{\chi}(a) \mathcal{G}_0(\chi) \right]. \quad (8)$$

page 6

## 4 The Artin-Weil Series [...]

### References

page 7

page 8

page 9

- [1] H. Davenport and H. Hasse, “Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen”, *Journal für die Reine und Angewandte Mathematik*, Volume 172, pp. 151–182 (1935)
- [2] André Weil, “Numbers of Solutions of equations in finite fields”, *Bulletin of the American Mathematical Society*, Volume 55, pp. 497–508 (1949)
- [3] André Weil, “Sur les courbes algébriques et les variétés qui s’en déduisent”, *Actualités scientifiques et industrielles*, no. 1041; Publications de l’Institut de mathématique de l’Université de Strasbourg, Volume 7 (1945), Hermann et Cie., Paris (1948)
- [4] André Weil, “Variétés abéliennes et courbes algébriques”, *Actualités scientifiques et industrielles*, no. 1064; Publications de l’Institut de mathématique de l’Université de Strasbourg, Volume 8 (1946), Hermann et Cie. Paris (1948)